CURVES OVER FINITE FIELDS

PAST, PRESENT, AND FUTURE

May 2021
L-functions in arithmetic statistics

$\mathbb{F}_q$ = finite field with $q$ elements

$C$ = smooth projective curve defined over $\mathbb{F}_q$ of genus $g$

What can we say about $\# C(\mathbb{F}_q)$ as $C$ and/or $q$ vary?

Weil conjectures

$Z_c(u) = \frac{P_c(u)}{(1-u)(1-Qu)}$

$\deg P_c(u) = 2g$ roots $121 = q^{1/2}$

$\# C(\mathbb{F}_q) = q + 1 - \text{Tr} (\text{Frob}_c)$

eigenvalues of $\text{Frob}_c$ are reciprocals of zeros of $Z_c(u)$
Today: distribution of \( \# C(F_q) \)

Book:

\[ N_q (g) = \sup \{ \# C(F_q); C \text{ of genus } g \} \]

3 main directions

- **geometric**: \( \{x \in \mathbb{Q}, \text{ let } g \to \infty \} \)

- **probabilistic**: \( \{x \in \mathbb{Q}, \text{ let } g \to \infty \} \)

- **arithmetic**: \( C/\mathbb{Q} \text{ reduce mod } p \text{ as } p \to \infty \)
Serre: Abelian $l$-adic representations and elliptic curves (1968)

Appendix A of Chapter 1

→ Peter-Weyl formulae

→ explicit connection to $L$-functions

→ compact groups
$G = \text{compact group}$

$(\tau_v)_{v \in \mathbb{Z}} \subset \text{Conj}(G)$ countable family

$\mathcal{S} = \text{irred reps of } G \text{ with character } \chi$

Assume $\tau \mapsto N\tau \in \mathbb{Z}_{\geq 2}$ function s.t.

$$\prod_{v \in \Sigma} \frac{1}{1 - N\tau^{-s}}$$

abs conv for $\text{Re}(s) > 1$,

has meromorphic cont. to $\text{Re}(s) > 1$

no zeros and no poles on $\text{Re}(s) = 1$ except

a simple pole at $s = 1$

Set $L(s, \mathcal{S}) = \prod_{v \in \Sigma} \frac{1}{\text{det}(1 - \tau(v) N\tau^{-s})}$

abs conv for $\text{Re}(s) > 1$, has meromorphic cont. to $\text{Re}(s) > 1$, no zeros and no poles on $\text{Re}(s) = 1$ except possibly at $s = 1$. 
Thm 1 (Serre)

(1) \( \# \{ v \in \Sigma : Nv \leq x \} \sim \frac{x}{\log x} \)

(2) \( \sum_{Nv \leq x} \chi(x_v) = c(x) \frac{x}{\log x} + \Theta \left( \frac{x}{\log x} \right) \)

where \( c(x) \) = order of the pole of \( L(s, \psi) \)

at \( s = 1 \)

Thm 2 (Serre)

Assume \( \exists C > 0 \) st. \( \# \{ v \in \Sigma : Nv = x \} < C + x \)

Then \( (x_v)_v \) are equidistributed wrt the normalized Haar measure on \( G \leftrightarrow \)

\( L(s, \psi) \) are holomorphic and nonzero

at \( s = 1 \) \( \forall \psi \) nontrivial irreducible rep of \( G \)
\[ \int_0^1 \frac{x^s}{\log x} \, ds \]

\[ \text{Re}(s) = 2 \]

Apply Wiener–Ihara
Geometric situation \[ \text{Fix } g, \text{ let } q \to \infty \]

Goal: distribution of \( \# C(\mathbb{F}_q) \)

where \( C \) curve of genus \( g \) / \( \mathbb{F}_q \)

and let \( q \to \infty \)

Birch (1968)
computes (even) moments of \( \text{Tr} (\text{Frob}_E) \)
for \( E = \) elliptic curve over \( \mathbb{F}_p \)

10th moment: \( C(p) \) appears

equidistribution results

Serre (1997): asymptotic distribution of eigenvalues of \( Tp \)
Katz–Sarnak (1998)

Deligne's equidistribution

\[ \downarrow \]

hyperelliptic curves / $\mathbb{F}_q$ of genus $g$

$\mathbb{F}_q \mathbb{F}_q^2 \mathbb{F}_q^3$ ... distribution of zeros of $Z_\infty$ approaches distr. of eigenvalues of random metrics in $USp(2g)$

Katz–Sarnak: hyperelliptic curves are generic in $\mathbb{F}_q$. 
General Katz--Sarnak philosophy:

distribution of eigenvalues of Frobenius for some family of curves approaches in the large \(g\)-limit the distribution of the eigenvalues of some ensemble of random matrices dictated by the monodromy group of the family.
Probabilistic situation: fix $q$, let $g \to \infty$

Goal: distribution of $\# C(q)$ for $C$ curve of genus $g$ as $g \to \infty$

- $\mathbb{P}$ - covers of $\mathbb{P}^1$

$l = 2$
Kurlberg - Rudnick (2009)
hyperelliptic

$l = \text{prime}$

- David, Feigon, Lalin (2010)
- David, Feigon, Kaplan, Lalin, Ozman, Wood (2016)

$$\# C(q) \sim X_1 + \cdots + X_{q+1}$$

$q \to \infty \quad \text{i.i.d. random var}$

$$X_i = \begin{cases} 0 & (l-1)/l(q+1)(q+2-1) \\ 1 & (l-1)/l(q+1)(q+2-1) \\ l & q/l(q+1)(q+2-1) \end{cases}$$
\[ S_3 \text{ curves (Wood, 2012)} \]

\[ 24/24 \times 24/24 \quad (\text{Lorenzo-Garcia, Meleleo, Millione, 2017}) \]

Poonen sieve (2004)

- plane curves \( B, \) Feigon, Lalin
- complete intersections \( B, \) Kedlaya
- semi-ample Bertini (Erman-Wood, 2012)
cohomological stability:

Ellenberg, Venkatesh, Westerland (2016)
→ Hurwitz spaces


\[ \# C(F_q) \quad \text{as } g \to \infty \]

\[ \text{Poisson distribution with mean } \]

\[ q + 1 + \frac{1}{q-1} \quad \text{(conjecture)} \]

Drinfeld-Vladut bound (1983)

\[ \limsup_{g \to \infty} \frac{N_g(E)}{g} \leq \sqrt{q} - 1 \]
Arithmetic situation
C/กา reduce mod p, let p → ∞
\[ L(s, C) = \prod_p \overline{L}_p(s, C) \]

- Sato-Tate conjecture (1960s)
- Yoshida: S-T over function fields (1973)
- Lang-Trotter (1976): generates interest in refined error terms in S-T
- V.K. Murty (1985): Lang-Trotter under GRH
- Serre (1994): gives the definitive formulation of the Sato-Tate conjectures in terms of motivic L-functions
- Fité, Kedlaya, Rotger, Sutherland (2010) formulate S-T for genus 2 curves
$g=1$: 3 distributions
  - non CM curves
  - CM
    over $\text{field } \mathbb{Q}_2$ and $\text{def } \mathbb{Q}_2$
    over $\text{an } \text{ext. } N_{\mathbb{Q}_2}(\mathbb{Q}_2)$

$g=2$: 52 distributions
  - 3 over $\mathbb{Q}$

$g=3$: 410
Barnet-Lamb, Geraghty, Harris, Taylor (2011)
Clozel, Harris, Taylor (2008)

Use Serre's method to reduce to proving mer coast + correct analytic properties for $L(s, \text{Sym}^k E)$

$E \text{ non CM} / F = \text{ totally real or CM}$

$L(s,E) = \prod_p \left( 1 - a_p \frac{q_p^{1-2s}}{q_p} + \frac{q_p^s}{q_p} \right)^{-1}$

$p \notin \{a_p, \phi \in \mathbb{I} \text{ p good red} \} \sim \mathcal{M}_S(t) \frac{x}{\log x}$

$\mathcal{M}_S(t) = \frac{2}{\pi} \int_0^t \sin^2 \theta \, d\theta$
B.-Kedlaya (2010)

$E_1, E_2$ non-isogenous non-CM elliptic curves $/k = \mathbb{Q}$ field

find a bound for $p$ of good red. st. $a_p(E_1) \neq a_p(E_2)$

$\rightarrow$ effective Sato-Tate (GRH)

$O((\log N)^2 (\log \log N)^b)$

$b = 2$ in 2010

$b = 0$ (Serre)

B., Tate, Kedlaya (2002?) (under GRH)

generalized to abelian varieties
Frobenius traws attaining Weil bounds

\[ E = \text{CM elliptic curve over } \mathbb{K} \]

\[ R(x) = \left\{ p \mid N_p < x \quad \alpha_p = \log N_p \right\} \]

Serre conjectured that \( ( \leq 2012) \)

\[ R(x) \sim \frac{4}{3\pi} \frac{x^{3/4}}{\log x} \quad (\star) \]

By Fité, Kedlaya under GRH

\[ R(x) \geq \frac{x^{3/4}}{\log x} \]

James Pollack (2017) : unconditional \((\dagger)\)